UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 88042 Horn Lane, Cottage Grove, OR and the Person of Matthew Blomquist, as described in Attachment A	)	Case No. 6:22-mc-984

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

88042 Horn Lane, Cottage Grove, OR and the Person of Matthew Blomquist, as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(1), (a)(2) and (a)(5) and (b)(1)	Transportation, Receipt, Distribution and Possession of Child Pornography

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jacob A. McPhie, FBI, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at _4:06pm_____a.m./p.m. *(specify reliable electronic means)*.

Date: 10/17/2022

/s/ Mustafa T. Kasubhai
Judge's signature

City and state: Eugene, Oregon

Mustafa T. Kasubhai, United States Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF JACOB A MCPHIE

Affidavit in Support of an Application Under Rule 41 for a Search Warrant

I, Jacob A McPhie, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation (hereinafter FBI), and have been since July 2018. My current assignment involves investigating child exploitation crimes. My training and experience includes investigating federal criminal violations related to child exploitation, and child pornography among other federal violations. I have gained experience through work relating to conducting these types of investigations. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 88042 Horn Lane, Cottage Grove, Oregon 97424 (hereinafter "Premises"), and the person of Matthew Blomquist, date of birth xx/xx/2000 as described in Attachment A hereto, for evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A. As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located at the Premises.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Target Offenses

4. I believe there is probable cause to believe that evidence of the following violations will be found in the places to be searched:

- Title 18, United States Code, Section 2252A(a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Title 18, United States Code Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. Title 18, United States Code, Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term child pornography is defined in Title 18, United States Code,

Section 2256(8).

Statement of Probable Cause[1]

5. As described more fully below, I have been involved in an investigation into the possible trading of child pornography by Matthew Blomquist. I received information tying Blomquist to several private chat rooms on Kik that were devoted to the trade of images of child sexual abuse. Separately, the Lane County Sheriff's Office received two separate Cypertips that linked Blomquist to the uploading of images of child pornography. Together with the Sheriff's Office, we have identified Blomquist and his current location at his mother' home on Horn Lane.

6. Between January 16, 2020, and May 4, 2020, during a proactive undercover investigation utilizing Kik[2] messenger, a messaging application, deputies of the Winnebago County Sheriffs posed as an adult female from Wisconsin. The Investigators entered multiple public groups which appeared to be created for individuals interested in child sexual abuse material. From these groups, they were added to multiple private and public groups within Kik

---

[1] Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP address*. The Internet Protocol address (or simply "IP address") is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet*. The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium*. A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

[2] Based on my training and experience I know Kik Messenger to be an application which allows for messaging and file sharing through the internet. A users Kik account can be accessed using the internet on any mobile device as long as the user has log in credentials for an account.

that had members openly engaging in the distribution of child sexual abuse material. One of these groups was named "Youn.gLand", the other was named "0" [zero].

7. The users bigclit420, and maxyp420 were members of these groups which have been established as child sexual abuse material sharing groups on Kik Messenger. Over the course of time spent within these groups, law enforcement observed multiple images and videos of child sexual abuse material had been shared with members of the groups.

8. The IP address used by both maxyp420 and bigclit420's Kik accounts was 172.223.216.37. A subpoena for to Charter Communications for subscriber information for that IP address with a lease start date of May 22, 2019, and end date of November 19, 2020, came back to: David Blomquist, 812 S. 3rd St, Cottage Grove, OR 97424. The emails associated with the account were blmq0014@charter.net, and matthew.blomquist@charter.net. Once the location of the possible suspect was identified as being in Oregon, the lead was forwarded to me to investigate.

9. Open-Source records checks show that David Blomquist is likely the father of Matthew Blomquist. This was confirmed by Michelle Blomquist, Matthew's mother, who said Matthew lived with his father at the premises during a conversation with a Lane County Sheriff's detective who used a ruse to attempt to locate Matthew Blomquist.

10. The email address associated with bigclit420 was macmore541@yahoo.com. A yahoo subpoena return showed that the recovery email for macmore541@yahoo was eclipse.ink15820@gmail.com, which is the same as the account email for maxyp420, one of the users that accessed the Kik groups that law enforcement identified as exchanging images of child sex abuse. A google subpoena return shows that the subscriber name for the google account

eclipse.ink15820@gmail.com was Matthew Blomquist.

11. Subpoena returns for an amazon account registered to macmore541@yahoo.com had a subscriber name on Matthew A Blomquist and a registered address of 812 S. 3rd St. Cottage Grove, Oregon. The account was created in July 2019. The phone number on file was 541-515-8582 which is consistent with the recovery phone number for macmore541@yahoo.com.

12. On September 21, 2022, Lane County Sherriff's Office Detective Zachary Lafoca was reviewing a case he had been assigned. The case which began with a tip from the Nation Center for Missing and Exploited Children (hereinafter referred to as NCMEC) generated on May 17, 2022. The NCMEC Internet Crimes Against Children (hereinafter referred to as ICAC) Cybertip was generated after receiving an alert from MediaLab/Kik regarding the uploading of apparent child pornography. The Cybertip was sent to the Lane County Sheriff's office who subsequently forwarded it to the FBI. The Cybertip states that 4 individual files containing pornography had been uploaded to Kik. Kik reported the username of the suspect was Maggiebaggy3. The email address associated with the account was matthewblomquist7162000@gmail.com.

13. Detective Lafoca viewed the four files attached to the ICAC Cybertip and provided the following descriptions:

File 1 and 3: (Duplicate, was uploaded on two occasions)

Filename: 97408f60-6efd-4120-ae63-affb8f2373e8.mp4

MD5: 6b365b0c8ae1073c9d5148d66708c269

Date of Upload: 03/13/2022 (18:17:27 UTC) and 03/13/2022 (22:38:21 UTC)

Description: This video is approximately 1 minute and 10 seconds long. The video shoes a pre-pubescent female child bent over on her knees with her fully exposed buttocks pointed upwards. The female is reaching back with her hands and physically separating her " butt cheeks" . There is an adult male positioned behind her sodomizing her by putting his erect penis in her anus while thrusting his hips. Towards the end of the video, the man positions the camera directly over the female' s anus, pointing downwards into her. The female briefly looks back at the camera and smiles before the video ends. The female has a small frame and does not have any body/pubic hair. The female has soft features on her face, and her hair is in "pig tails" . The male subject' s leg in the video appears to be almost the same side as the female' s torso. The video is being filled in what appears to be a concrete shack, likely in another country. I estimate the female' s age in this video to be about 10 years old.

File 2:

Filename: ccd0e9e6-bbed-473b-b494-4da32c5e009f.mp4

MD5: 77a291f25f534544f1f66ad8447d5988

Date of Upload: 03/15/2022 (04:06:15 UTC)

Description: This video is approximately 2 minutes long. The video starts by showing an unclothed pre-pubescent female squatting over a camera. The female is rubbing her fully exposed vagina and pulling it open with her fingers. The female has no body or pubic hair, and her vagina does not appear fully developed. The camera pans up and shows two fully nude prepubescent females in what appears to be a bedroom. Neither female had any body hair. Both had small undeveloped breasts and nipples. The video then shows the

two females putting their clothes on while looking into the camera. Towards the end of the video both females pull their pants down and bend over, putting their buttock' s towards the camera while shaking them in a provocative manner. I estimate the females in this video to be between 9 and 13 years old. The word " OMEGLE.com" is superimposed on the bottom of the screen. Omegle.com is an online video chatting website, indicating whomever the females connected to on the website was filming his or her interactions with them.

File 4:

Filename: 4faa2bfe-6f27-4dae-8efc-d0b53a37cbff.mp4

MD5: d0174d38215a4ee6ad859b35730574cd

Date of Upload: 03/15/2022 (03:45:48 UTC)

Description: This video is approximately 41 seconds in length. The video shows a pre-pubescent female on her hands and knees on what appears to be a bed. The females face his hidden, as she is putting it against the bed. Her pants and underwear are removed, and her lower half is fully exposed. There is an adult male subject behind her sodomizing her by putting his erect penis in her anus while thrusting his hips. The female has a very small frame and appears to have no body hair. The male' s penis is about 1/4 th the size of the female entire lower body. I estimate the females age to be between 7 and 10 years old.

14. Oregon Department of Justice sent Century Link a subpoena for subscriber information for the IP address used to upload the images. Century Link responded to the

subpoena on July 22, 2022. The response indicates the IP Address, 63.155.77.193, was assigned to Tim Leach at 37457 Row River Road, Dorena, Oregon 97434.

15. After reviewing the uploaded content, Det. Lafoca began searching for information about Matthew Blomquist, based on the name in the email address, and Tim Leach, based on the IP address location. A Matthew Aaron Blomquist date of birth XX/XX/2000 was located in the Lane County Sheriff' s Office local records system. Blomquist had a listed address of 812 South 3rd Street in Cottage Grove and a listed phone number of (541) 510-7513. Records checks for Timothy Lewis Leach, date of birth XX/XX/1974 in the Lane County Sheriff' s Office local records system showed Timothy had a listed address of 37457 Row River Road in Dorena, the same address listed on the Cybertip.

16. On September 21, 2022, Det Lafoca drove to Leach's residence at 37457 Row River Road to conduct surveillance on the residence. As Lafoca was heading to the property, he learned that separate Cyber Tip, Cyber Tip 114362571, had been located pertaining to the first. The address associated with the tip was also 37457 Row River Road. The report indicated over 30 files containing child pornography were uploaded to Media Lab/Kik from an account with the username Matthew.b1369 on December 27, 2021. The email address associated with the Kik account is matthew.blomquistsoccer10@gmail.com. This email is also used in a skype account with the display name of Matthew. During the surveillance, he found the address to be very rural and obscured from the street by a large fence. He was able to confirm that the Wifi accessible near the house was password protected. Additionally, there was no cellular service in the area which meant anyone using a digital device would be required to use the internet.

17. Det. Lafoca viewed all 30 files and provided the following descriptions for some

of the files received:

File 6:

Filename: 8bb147d8-987d-4263-8cc2-b47bdeddddfe.mp4

MD5: 4cc77b9b0618768d1e5c0333ff788b97

Date of Upload: 12/02/2021 (03:54:09 UTC)

Description: This video is about 20 seconds long. I believe both the victim and suspect in this video are the same subjects as it file 5. The video depicts a fully unclothed pre-pubescent female lying on her back on a bed. The victim' s knees are pulled up to her chest, and her anus and vagina are fully visible. The suspect if physically holding the victim in place. The suspect, a fully unclothed adult female, is wearing a " strap-on dildo." The suspect begins penetrating the victim' s anus with the dildo while thrusting her hips. A few seconds after the penetration starts, the victim can be seen trying to kick at the suspect and push away from her with both her hands and feet. The suspect aggressively grabs the victim' s legs and forces her flat on the bed. The suspect continues sodomizing the victim and the video ends a short time later. I again estimate the age of the victim in this video to be between 8 and 10 years old.

File 10:

Filename: 507fa567-aefa-43d2-9b5f-ff50f8d42a6f.mp4

MD5: 7205fb917a479fb40379ceaf2838deca

Date of Upload: 12/02/21 (03:16:10 UTC)

Description: This video is about two minutes in length. The video depicts a pre-pubescent female lying in her back. The female' s pants and underwear have been removed and her

vagina is fully visible. The female victim is pulling her shirt up and one of her undeveloped breasts are exposed. The victim does not have any body hair or pubic hair. An apparent adult male is standing in front of her and is rubbing his erect penis on the victim' s vagina. The suspect then begins attempting to insert his penis in the victim' s vagina but appears to be physically unable to fully insert it. I estimate the age of the victim in this video to be between 5-8 years old.

File 11:

Filename: a7ec2669-6ae7-498f-8edb-d92fdc79884d.mp4

MD5: fada72fca34b0208666fd2d4a17d6d8e

Date of Upload: 12/02/2021 (04:11:32 UTC)

Description: This video is about 23 seconds in length. The video depicts a pre-pubescent female child lying on her back on what appears to be a table. The video starts with the female looking at the camera. The female appears to be between 3 and 5 years old and is wearing a shirt with children' s cartoon characters on it. The camera pans down and an adult male can be seen sodomizing the victim by putting his erect penis in her anus while thrusting his hips. The suspect can be seen at times, physically holding the females' legs apart. The female has no body hair or pubic hair.

File 12:

Filename: c5c05c66-e197-419c-aeb8-bfdf714b37eb.mp4

MD5: 998afb8177823b68050801ca5aa2da9b

Date of Upload: 12/02/2021 (03:55:46 UTC)

Description: This video is about one minute and 30 seconds in length. The video appears

to be a screen recording on an I-Phone. The video begins by showing a female child asleep on a bed. The female' s face is clearly visible and is that of a child. The female is lying on top of " Little Mermaid" bed sheets. A male with an erect penis is seen standing over the female. The male begins masturbating by rubbing the tip of his penis. Moments later, the male ejaculates onto the females face and mouth while she is still asleep. The male suspect zooms the camera in on the female, showing his ejaculate on her lips. Another video clip plays showing the same female asleep on the same bed. The video again shows the male subject ejaculating on her face. A third video clip of the same victim then starts. In this clip the male subject is rubbing his erect penis on the victim' s mouth while she is asleep. A fourth video clip starts. Showing the same female asleep on her bed while the male subject ejaculates onto her face. I estimate the age of the female in the four video clips to be between the age of 7 and 10. In the above-mentioned videos the female is wearing small square earrings in at least one of her ears. A fifth video clip starts a short time later, showing the same female child performing oral sex on a male' s erect penis by putting the tip of his penis in her mouth. The female in the fifth video is wearing the same earrings as previously stated. After the fifth video ends, a photograph of what appears to be a prepubescent male child sucking on the nipple of an adult female shows on the screen. The male victim is seen rubbing the suspects vagina. The male does not appear to have any body hair or pubic hair. His face and torso look like that of a child. I estimate the age of the male victim to be between the ages of 9-13 years old.

///

///

Ascertaining the Location of Blomquist

18. The following day, September 22, 2022, Det Lafoca called Timothy Leach. After Det. Lafoca used a ruse for the reason for the call, Timothy explained that Matthew had been living at his house around 6 months prior (around March 22, 2022), but he no longer lived there. Timothy said Matthew moved back in with his mother, Michelle Blomquist. Timothy provided a phone number for Michelle. Timothy was not positive exactly when Blomquist had moved out but remembered it to be around the beginning of 2022.

19. Det. Lafoca then called Michelle using the same ruse. He asked Michelle if Matthew used to live with Timothy Leach. Michelle told Lafoca he did, and indicated Timothy was Matthew' s uncle. Michelle explained Matthew didn't live anywhere full time, and he " couch surfed" looking for places to stay. Michelle advised that as of September 22, 2022, Matthew was staying at his father' s house, located at 812 South 3rd Street in Cottage Grove. Michelle also said that Blomquist was living with Timothy around the beginning of 2022.

20. Det. Lafoca continued to try and identify a residence for Matthew and eventually learned he was back at his mother's home. On October 12, 2022, Det. Lafoca made contact with Matthew Blomquist, again using a ruse, at 88042 Horn Lane, Cottage Grove, Oregon 97424, which he had previously identified as Matthew's mother's home. Blomquist told Lafoca that he lived there with his mother Michelle. Blomquist gave a phone number ending in 1229 which Det. Lafoca called after the interaction to confirm that it worked and that Blomquist was the primary user. Blomquist gave an email of matthewblomquist2000@gmail.com. Blomquist told Lafoca that he had been living there with his mother for a few years. While that phone number is not the same as associated with the prior police reports, a review of the Kik tips shows

that a different device was used for each upload. This is consistent with someone upgrading or purchasing a new phone. Kik is an application that requires a log on, and it can be downloaded to a new phone with the same login, and it will maintain stored material. A user can only be logged into a Kik account on one device at a time, and the application forces any other devices off the account when a new log in occurs. Kik can operate using cellular data or Wi-Fi. I am aware that using Wi-Fi, which can often be accessed for free, can preserve cellular data which typically costs money. I am also aware that when someone accesses Wi-Fi at a location, it can leave behind a footprint that can be traced. Given Blomquist's families statements regarding his transient nature, it is highly likely that he is accessing Kik and child pornography at multiple locations, including where he attests to be living currently. Given Blomquist's prolific transmission of child pornography, occurring for over a year, all of which appears to have happened on Kik, and across multiple residences, which he is said to have lived at, it is likely that he is using his cell phone to store images or child pornography. According to the Kik returns, that device has changed throughout the year, and it is very likely that the old device(s) are currently stored at his residence.

Electronic Records

21. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

22. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know Kik requires the use of a digital device. I also know that possessors of child pornography keep their images in a place they can ensure their security, either through hiding them or by securing them on their person. It is likely the uploaded images are either still on the subject's device or have been transferred to a media storage device for safekeeping. I also know that:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital device

users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d. Based on actual inspection of other evidence related to this investigation, including search warrant returns, subject confessions, and subpoena returns, I am aware that digital devices were used to generate, and store, content used in the purchase and transmission of Child Pornography. Thus, there is reason to believe that there is a digital device currently located on the Premises.

23. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of

peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a digital device to commit a crime such as to transport, distribute, receive and possess child pornography, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I

believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

24. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

25. Because several people share the Premises as a residence, it is possible that the Premises will contain digital devices that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the warrant applied for would permit the seizure and review of those items as well.

26. I know from my training and experience, as well as from information found in publicly available materials that some digital devices offer their users the ability to unlock the device via the use of a fingerprint, thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. These features are commonly referred to as biometric authentication and their availability is dependent on the model of the device as well as the operating system on the device. If a user enables biometric authentication on a digital device, he or she can register fingerprints to unlock that device.

27. In some circumstances, biometric authentication cannot be used to unlock a device, and a passcode or password must be used instead. These circumstances include: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; (3) too many unsuccessful attempts to unlock the device via biometric authentication are made; (4) when too many hours have passed since the last time the device was unlocked; and (5) when the device has not been unlocked via biometric authentication for a period of time and the passcode or password has not been entered for a certain amount of time.. Thus, in the event law enforcement encounters a locked digital device, the opportunity to unlock the device via biometric authentication exists only for a short time.

28. The passcode or password that would unlock digital devices found during the search of the Premises are not known to law enforcement. Thus, it will likely be necessary to press the fingers of the potential users of the digital devices found during the search of the Premises to the device's sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via biometric authentication is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

29. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via biometric authentication, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that

in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require different individuals in the Premises to press their fingers against the sensor of the device found during the search of the Premises in order to attempt to identify the device's user(s) and unlock the device(s) via biometric authentication. Based on these facts and my training and experience, it is likely that Matthew Blomquist is one user of the device(s) and thus that his fingerprints are among those that are able to unlock the device.

30. I therefore request that the Court authorize law enforcement to press the fingers, including thumbs, of Matthew Blomquist found at the Premises to the sensor of the device(s) found at the Premises for the purpose of attempting to unlock the device(s) via biometric authentication in order to search the contents as authorized by this warrant.

Nature of Examination

31. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

32. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the

government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

33. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

34. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

35. If a computer or storage media contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain that computer or storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

36. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to

questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

37. Based on the foregoing, I have probable cause to believe, and I do believe, that Matthew Blomquist committed the Target Offenses, and that contraband and evidence of those offense(s), as described above and in Attachment B, are presently located at the Premises, or on Blomquist's person which are described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the Premises described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

38. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Amy E. Potter. I was informed that it is AUSA Potter's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

/s/ Jacob McPhie, per rule 4.1

JACOB A. MCPHIE
Special Agent, Federal Bureau of Investigation

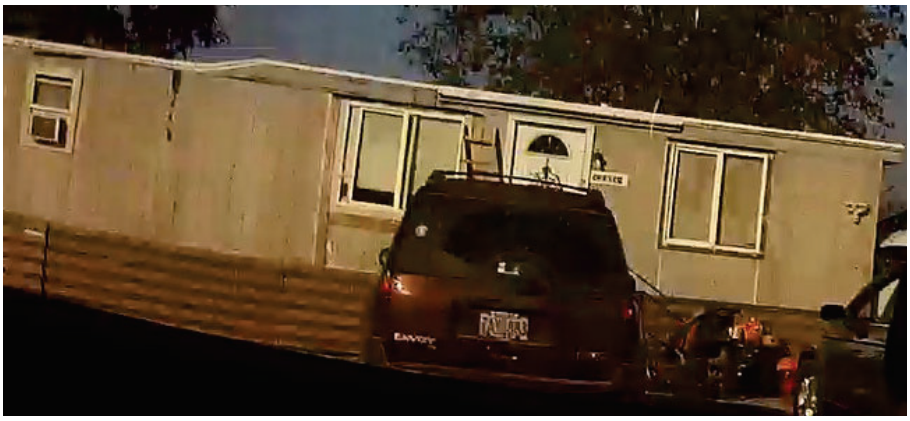
Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 4:06pm a.m./p.m. on October 17, 2022.

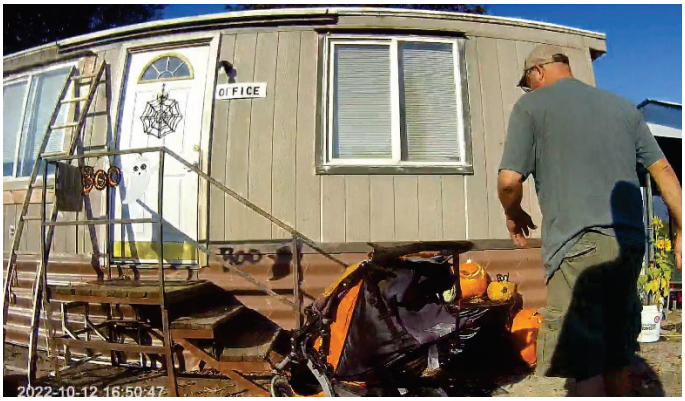
HONORABLE MUSTAFA T. KASUBHAI
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is 88042 Horn Lane, Cottage Grove, Oregon 97424, further described as a grey in color single story, single family residence with a white door and the word "OFFICE".





(image current as of 10/12/22)

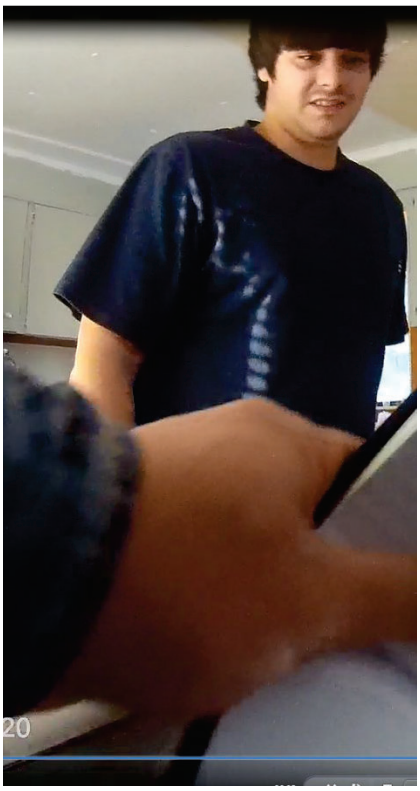
/

/

/

/

The person of Matthew A Blomquist, a white male, date of birth 7/16/2000, who is described in his driver's license as 5'08" tall.



(image current as of 10/12/22)

ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the premises located at 88042 Horn Lane, Cottage Grove, Oregon 97424 as referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), transportation, receipt, distribution, possession and access with intent to view child pornography. The items to be seized cover the period of through the date of the execution of the search warrant.

1. The items referenced above to be searched for, seized, and examined are as follows:

a. Any and all records, documents, or materials, including correspondence, that pertain to the production, possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

b. All originals and copies (physical or digital) of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

c. Any and all motion pictures or digital video clips of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256; video recordings which are self-produced and pertain to sexually explicit images of minors; or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

d. Any and all records, documents, or materials which include offers to transmit, through interstate commerce by any means (including by computer), any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

e. Any and all records, documents, or materials relating to the production, reproduction, receipt, shipment, trades, purchases, or transactions of any kind involving the transmission, through interstate commerce (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

f. Any and all records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, and e-mail messages.

h. Any records, documents, or materials referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, receiving, or transporting child pornography, including chat logs, call logs, address book or contact list entries, and digital images sent or received.

i. Computers, storage media, or digital devices used as a means to commit the violations described above, including accessing and viewing child pornography.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence

of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the

operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.